

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRAD RAFFENSPERGER, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

DECLARATION OF J. ALEX HALDERMAN

J. ALEX HALDERMAN declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. Plaintiffs have discussed the need to analyze two distinct kinds of data from Georgia's election system:

- a. Copies of GEMS database files from particular counties and from the Secretary of State's office. These are Microsoft Access files that contain the ballot layouts and other election configuration data used to program voting machines, as well as the election results from individual machines used to produce overall vote tallies.
- b. Copies of the hard drives from election management computers. These computers are operated by the Secretary of State's office and by counties, and include GEMS servers (used for preparing voting

machine programming and for tabulation), ExpressPoll data servers (used for preparing electronic poll book programming), and workstations that employees use to access these servers.

2. The hard drives from election management computers may contain sensitive information that is necessary to keep confidential, such as personally identifying information about voters and undisclosed information about how these computers are secured. In contrast, GEMS database files are not sensitive. They are routinely made public in other states, and their disclosure in Georgia would not create any new security risk to the election system.

3. As a first step in their analysis, Plaintiffs seek to examine only the GEMS database files. Since these files are not security sensitive, the State should be able to produce them with or without a protective order. During the June 28 telephone conference, I understood the Court to be proposing greater protections for an analysis that would include both the GEMS database files and the election management hard drives. Such protections are unnecessary for an analysis of only the GEMS database files.

4. Even if the court concludes that the GEMS database files need to be protected from disclosure, the access conditions proposed by the State Defendants are not well tailored to the state's own security goals, and they would severely impair Plaintiffs' ability to perform the examination.

5. State Defendants have proposed conditions for protecting the database files that are even more restrictive than the state's own procedures for protecting its election management computers. These computers are the nerve center of the entire election system and warrant a far higher level of precaution than mere copies of GEMS database files. Michael Barnes, Director for the Center for Election Systems at the Secretary of State's Office, has testified that multiple employees have simultaneous access to the election management servers via a local computer network, and that workers regularly use USB sticks and CDs to copy files into and out of the air-gapped network. These actions would be prohibited by the state's proposed access conditions.

6. State Defendants have articulated two distinct security goals: (1) protecting confidential information in the GEMS database from unauthorized disclosure; and (2) "allowing a review in the Secretary of State's own environment without introducing anything foreign into that system." Neither goal necessitates the proposed access conditions.

7. The State is right to be concerned about the general threat of malware infiltrating its election system. However, in the present context, where Plaintiffs seek only to examine a *copy* of data from the election system, this risk can be eliminated simply by performing the analysis in a completely separate facility from the state's, such as in a secure environment at the University of Michigan or at

Morrison & Foerster. Should the Court conclude that the analysis must take place in a facility controlled by the Secretary of State, the risk of spreading malware to state systems can still be more straightforwardly eliminated: Plaintiffs can conduct their analysis in an isolated room with no connection to any state computers or networks, and the state can ensure that no computer or storage device used in the examination is ever later connected to a state system.

8. Similarly, there are far less burdensome ways to mitigate the risk of unauthorized data disclosure. For instance, the Court could simply impose a protective order. Should the Court determine that additional security measures are necessary, Plaintiffs' experts and attorneys could further agree to analyze the data only on air-gapped systems in secure environments at their own facilities, to maintain the data on encrypted storage devices, and to destroy or securely erase all such storage upon final disposition of the matter.

9. The State Defendants' proposed access conditions would severely impede an effective examination. The state proposes to provide a single computer with the same software environment that Georgia counties use to run GEMS. However, GEMS runs only under obsolete versions of Microsoft Windows, and an efficient analysis calls for the use of modern software. More recent operating system software is also more secure than obsolete versions, so the state's proposal would only serve to increase security risks.

10. Moreover, the state proposes to provide only Microsoft Access and to prohibit Plaintiffs from installing any other software. An effective examination will require additional software tools, such as specialized software to examine the low-level structure of the database, to compare multiple versions of the database, to check the data for consistency, and so on. Plaintiffs' experts will not be able to determine the full set of software tools that are necessary for their analysis until the examination is underway. With appropriate controls, software and data can be copied into the secure environment without creating any risk that confidential data will be copied out, and so the state's proposed restriction would serve only to impede the analysis.

11. States Defendants' also propose to provide only supervised data access, and they demand copies of all notes taken during the review except for attorney work product. These restrictions would impede an effective examination by making it difficult for Plaintiffs' experts to privately confer in order to develop and test hypotheses about the data.

12. States Defendants' additionally propose to conduct the analysis in a state facility in Atlanta, and to limit the analysis to a single computer workstation. These restrictions are unnecessary for security and would greatly impede the efficiency of the examination. Even if Plaintiffs had unrestricted access to the data, a complete examination of the GEMS database files is likely to take weeks of effort by a team of people. Several factors make this analysis more complicated than a

routine forensic review: the size of the data; the age of the computer software involved; the specialized nature of the GEMS application; and the potential that the GEMS databases files have been altered in an attack by hostile nation-states.

13. In order to analyze the data efficiently, Plaintiffs' should be allowed to access the data from multiple air-gapped computers, so that several people can work at the same time. Limiting the analysis to a single computer would multiply the duration of the effort.

14. Similarly, requiring that the analysis be performed at the state's facility serves no security purpose, since Plaintiffs' can establish equivalently secured environments at their own facilities while reducing the burden and expense of extended travel. I am prepared to set up a separate, secure facility at the University of Michigan, in which only I and Plaintiffs' other experts and attorneys would be able to access the data.

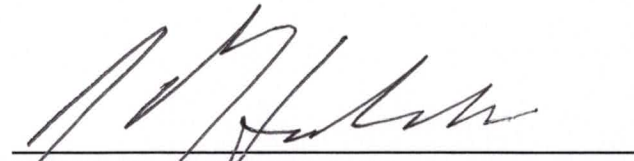
15. My lab at the University of Michigan has a long track record of safeguarding data that is much more sensitive than the GEMS database files. In the course of our research activities, we handle copies of computer viruses, ransomware, and other malicious software that, if released, could damage other people's systems; source code for exploiting unpatched vulnerabilities in widely used computer software; undisclosed vulnerabilities in cryptographic protocols used by billions of people; personally identifying information about research participants subject to

institutional review board controls; and functional vote-stealing software that targets the AccuVote TS and TSX DREs. We have developed security controls to protect such sensitive information, and to my knowledge, we have never had a data breach resulting in its disclosure.

16. Should the Court determine that the highest level of security is warranted for the GEMS databases, I would propose to adapt the security plan developed by the Secretary of State of California for that state's 2007 "Top-to-Bottom Review" of election system security. During that analysis, in which I served as an expert, the state commissioned independent computer security experts to examine the complete software source code for voting machines and election management systems used in the state, including the source code for the GEMS software. Voting system source code is far more sensitive than GEMS database files, since access to the source code could allow an attacker to more easily discover and exploit vulnerabilities in the software. The California Secretary of State and her security experts developed a security plan that would strongly protect the source code from disclosure while facilitating an effective examination. In contrast to the State Defendants' proposed access conditions, the California security plan would permit experts to efficiently conduct the examination at their own secure facilities and to use the computer systems and software tools that they determine to be

necessary for an effective analysis. The plan is available online at <https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/source-code-security-plan.pdf>.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 3rd day of July, 2019 in Ann Arbor, Michigan.



J. ALEX HALDERMAN